


Secrétariat général de la défense
et de la sécurité nationale

Guerre en Ukraine

Trois années d'opérations informationnelles russes

Version : 1.0

VIGINUM

Synthèse

Février 2025

TLP:CLEAR

SOMMAIRE

1. CONTEXTE

Depuis le 24 février 2022, l'invasion à grande échelle du territoire ukrainien par les forces armées de la Fédération de Russie a été accompagnée d'une offensive d'envergure du dispositif d'influence informationnelle russe. Cette offensive, qui s'inscrit dans le cadre de stratégies de « confrontation informationnelle » lancées par l'État russe dès le début des années 2000, cible tant la population ukrainienne que les audiences internationales, dont française. Son objectif principal est de légitimer le bien-fondé de « l'opération militaire spéciale » en Ukraine, en la présentant comme une action défensive face à la prétendue agressivité d'un État ukrainien soutenu par « l'Occident collectif ».

Pour ce faire, les acteurs du dispositif d'influence russe et leurs modes opératoires informationnels (MOI)[1] utilisent un large panel de tactiques, techniques et procédures (TTP), telles que l'animation d'avatars sur les réseaux sociaux pour diffuser du contenu de propagande, la création de faux sites *web* d'information, l'instrumentalisation de groupes de la société civile et de partis politiques étrangers, ou encore l'amplification, dans le champ informationnel, d'actions menées dans le champ physique.

Dès le 2 mars 2022, le Conseil de l'Union européenne a mis en place des « mesures restrictives » visant à contrer les « actions de propagande » que conduit la Russie pour « justifier et soutenir son agression », qui ont entraîné la suspension des activités de diffusion des médias transnationaux russes *RT* et *Sputnik*. Ces mesures, qui ont permis de réduire considérablement l'audience de ces deux médias, ont provoqué une forme de « clandestinisation » des activités de *RT* et *Sputnik* et l'apparition de nouveaux modes opératoires informationnels s'additionnant à ceux préexistants au 24 février 2022. Ces mesures n'ont par ailleurs ciblé que la partie visible et assumée d'un dispositif d'influence informationnelle russe composé d'une multitude d'acteurs, et dont la France constitue l'une des principales cibles.

Ainsi, au titre des attributions qui lui sont confiées par l'article 3 du décret n°2021-922 du 13 juillet 2021, VIGINUM a ouvert, dès le 24 février 2022, une opération dédiée à la recherche d'ingérences numériques étrangères liées à la guerre d'agression menée par la Russie contre l'Ukraine et aux répercussions de cette dernière dans le débat public numérique français. Dans ce cadre, VIGINUM a caractérisé l'activité de plusieurs modes opératoires informationnels russes comme constituant des ingérences numériques étrangères (INE).

Les MOI actifs sur le sujet de la guerre en Ukraine sont présentés ci-dessous selon la zone géographique et les audiences qu'ils ciblent de manière prioritaire : le territoire national français, le continent européen, l'Ukraine et les territoires occupés par l'armée russe, ainsi que le continent africain. Ces modes opératoires ont été attribués publiquement à des acteurs étatiques russes, mais également à des acteurs privés auxquels le gouvernement russe sous-traite l'exécution d'opérations informationnelles, ou qui financent eux-mêmes des opérations dans le but d'en tirer des bénéfices financiers ou politiques.

Malgré les moyens techniques, financiers et humains considérables alloués par l'État russe à son dispositif d'influence informationnelle, VIGINUM considère que la portée des campagnes conduites par les MOI russes présentés dans ce rapport reste relativement limitée, notamment en raison des nombreuses erreurs techniques commises par leurs opérateurs et de la mauvaise qualité des contenus produits. Par ailleurs, si, à de rares exceptions près, ces MOI sont parvenus à rendre viraux certains des récits trompeurs initialement destinés à des audiences internes avant d'être réemployés vers l'étranger, ils ont avant tout cherché à amplifier des lignes de fracture politique liées à la guerre et à instrumentaliser des polémiques préexistantes.

S'il n'a pas vocation à restituer l'exhaustivité de la connaissance de VIGINUM sur les acteurs de la menace informationnelle russe, ce rapport propose de présenter sous la forme d'une synthèse les principaux MOI observés depuis trois ans, dont la majeure partie est apparue en corollaire de la guerre d'agression menée par la Russie en Ukraine.

[1] VIGINUM définit un mode opératoire informationnel (MOI) comme un ensemble de comportements, d'outils, de tactiques, techniques et procédures et de ressources adverses mis en œuvre par un acteur ou un groupe d'acteurs malveillants dans le cadre d'une ou de plusieurs opérations informationnelles numériques.

2. MODES OPÉRATOIRES INFORMATIONNELS CIBLANT LA FRANCE

La France, par son statut de membre permanent du Conseil de sécurité de l'ONU et sa politique affichée de soutien économique et militaire à l'Ukraine, fait l'objet d'un ciblage particulièrement agressif et persistant des acteurs de la menace informationnelle russe. Ce ciblage s'est sensiblement intensifié depuis les déclarations du président de la République française le 26 février 2024, qui indiquaient que l'option éventuelle d'envoi de troupes sur le territoire ukrainien n'était pas exclue. Largement instrumentalisées par le dispositif d'influence russe, ces déclarations ont fait l'objet de plusieurs campagnes coordonnées visant à présenter la France comme isolée et responsable d'une escalade du conflit, à décrédibiliser les forces armées françaises et à mettre en scène une prétendue opposition de la population française à cette position.

2.1 *RRN*, un MOI persistant à l'efficacité limitée

Depuis le printemps 2022, le mode opératoire informationnel *RRN* (*Reliable Recent News*, aussi connu sous les noms de *Doppelgänger* ou *Ruza Flood*) tente de saper le soutien occidental à l'Ukraine en ciblant notamment la France et d'autres pays européens. Pour ce faire, *RRN* s'appuie sur un réseau de plusieurs centaines de sites de désinformation, que VIGINUM regroupe dans deux catégories :

- des sites *web* usurpant l'identité de médias (*Le Monde*, *The Washington Post*, *Der Spiegel*, etc.) et d'institutions (OTAN, ministère de l'Europe et des Affaires étrangères français, etc.) *via* des techniques de typosquattage ;
- des pseudo-médias francophones spécialisés sur des thématiques ciblées (sport, « *lifestyle* », actualités européennes, etc.) diffusant des articles à la ligne éditoriale anti-ukrainienne.

Les opérateurs de *RRN* tentent de promouvoir ces ressources sur les plateformes en ligne (principalement sur *X*, *Facebook* et *TikTok*) en utilisant des réseaux de comptes et de pages inauthentiques, et en amplifiant leur visibilité *via* des contenus sponsorisés. Bien qu'une baisse notable d'activité ait pu être observée sur *Facebook* à partir de l'été 2024*, RRN* continue de coordonner et d'alimenter deux réseaux constitués de centaines de milliers de comptes inauthentiques sur la plateforme *X*.

Les comptes du premier réseau publient dans l'espace réponse de comptes *X* des URL redirigeant vers les sites administrés par le MOI, tandis que ceux du second diffusent de courtes vidéos anti-ukrainiennes en utilisant les *hashtags* « tendances » de la plateforme dans l'espoir d'améliorer le référencement de leurs publications. Ce second réseau, dénommé *Revolubots* par VIGINUM depuis le printemps 2023, est également connu en source ouverte sous le nom d'*Undercut*.

Le 4 septembre 2024, *RRN* a fait l'objet d'une attribution publique par le département de la Justice américain (DoJ). Selon le DoJ, le MOI aurait été directement commandité et supervisé par le premier directeur adjoint de l'Administration présidentielle russe (AP), Sergueï KIRIENKO. Il aurait été mis en œuvre par l'*Agence de design social* (*ASP*, ou *SDA*) et *Struktura*, deux entreprises russes de marketing numérique, ainsi que par l'organisation autonome à but non lucratif *ANO Dialog*, chargée par l'AP de la propagande à destination des audiences russes.

Depuis trois ans, *RRN* poursuit ses activités malgré les multiples attributions, dénonciations publiques et mesures d'entrave dont il a fait l'objet. Cette persistance peut s'expliquer en partie par les stratégies de contournement de modération mises en place par le MOI, qui exploite notamment un système de redirection historiquement lié à l'écosystème cybercriminel pour tromper les algorithmes de détection des plateformes.

Alors que l'efficacité des opérations conduites par le MOI peut être considérée comme faible, des documents internes de la société *ASP* publiés dans la presse suggèrent que son fondateur, Ilya GAMBACHIDZE, tirerait profit des dénonciations et attributions publiques dont a fait l'objet *RRN*. Elles lui permettraient en effet d'exagérer les capacités de sa société à influencer les audiences étrangères, notamment lors des dernières élections européennes, et, ce faisant, d'en tirer également des bénéfices

financiers et politiques. Selon le chercheur Thomas RID, « l'objectif principal [d'*ASP*] n'est pas d'influencer les citoyens des pays adverses, mais de persuader la bureaucratie russe que son entreprise était efficace dans le but de décrocher de nouveaux contrats ou de renouveler son budget ».

2.2 *Matriochka*, un MOI ciblant les médias et *fact-checkers*

Depuis 2022, l'un des objectifs du dispositif d'influence numérique russe est de dénigrer les médias et la communauté des *fact-checkers* en les accusant de disséminer de fausses informations sur le conflit. Cette tactique, observée à de nombreuses reprises depuis l'annexion illégale de la Crimée en 2014, a notamment motivé la création du site « *War on Fakes* » par *ANO Dialog* dès le 1er mars 2022, ou encore le lancement d'un « réseau international de *fact-checking* » par des acteurs du dispositif d'influence russe en novembre 2024.

Actif *a minima* depuis le mois de septembre 2023, le MOI connu publiquement sous le nom de *Matriochka*, *Storm-1679* et *Overload* a pour objectif de discréditer et de perturber le travail de la communauté de *fact-checking*, au sein de laquelle plusieurs organisations françaises ont été visées. Il consiste en la publication coordonnée de faux contenus primo-diffusés sur *Telegram* (reportages, captures d'écran, graffitis) dans l'espace réponse des publications de comptes *X* de médias, de personnalités et de cellules de *fact-checking*. Les opérateurs de *Matriochka* interpellent directement leurs cibles sur *X* ou *via* leur adresse électronique pour leur demander d'enquêter sur ces faux contenus.

Schéma d'attaque du mode opératoire informationnel *Overload*

OVERLOAD

STORM-1679

Faux contenus

- reportages, captures d'écran, photos de graffitis, etc.
- usurpant l'identité de médias et d'organisations occidentales
- primo-diffusés sur des chaînes *Telegram* russophones

От подписчика: причина повышенного содержания бактерий в Сене - санкции против России.

Из-за санкций в отношении России некоторые комплектующие очистительных сооружений были заменены на польские. Парижу не удалось закупить технические устройства, попавшие в подсанкционный список, и был вынужден искать ближайшие альтернативы.

На обновление 2 из 5 уровней очистительных сооружений на Сене с использованием польских комплектующих было затрачено боле 1,5 млн евро.

1,5 млн евро в трубу. КУРВА!

https://www.nbcnews.com/news/olympics/paris-olympics-river-seine-pollution-cancel-triathlon-swimming-rcna147142

MATRIOCHKA

Comptes *seeders* — Comptes *quoters*

reply

The reason for the increased bacteria content in Sena is the sanctions against Russia.

Apr 15, 2024 · 7:35 AM UTC

The latest news makes me cringe

Apr 15, 2024 · 8:00 AM UTC

reply

Polish components can't cope with the cleaning of the Seine

Apr 15, 2024 · 7:49 AM UTC

I don't understand how long this is going to go on????

Apr 15, 2024 · 8:00 AM UTC

envoyés par *mail* à des médias et cellules de *fact-checking*

[redacted]
check the news
To: Check First
1 May 2024 at 16:34

Hello. Could I have your attention, please? The news that is being spread in the Russian media. The videos are very similar to real news. It is not clear to believe or not to believe. I will attach some links where there are many opinions.

The news is as follows:

- "Facebook and Twitter have been attacked by Ukrainian bots working in favor of Yermak."
- "Statistical agencies in Europe have recorded a drop in Zelensky's rating to the level of 2019."
- "Ukrainian media holding 1+1 Media Group has overtaken FOX in the number of employees!"

https://t.me/kotreal/30267, https://t.me/kotreal/30263, https://t.me/kotreal/30266, https://t.me/energynewz/99338, https://t.me/sheyhtamir1974/84560

Sources : @antibot4navalny, Check First, Microsoft, Viginum

Figure 1. Schéma d'attaque du MOI Overload

Les faux contenus usurpent généralement l'identité de personnalités et de médias nord-américains ou européens, notamment français. L'identité de VIGINUM a également été usurpée à la suite de la publication, en juin 2024, d'un rapport technique sur *Matriochka*. Plus récemment, le MOI a diffusé des montages visiblement générés à l'aide d'une intelligence artificielle qui usurpaient le logo d'universités et la voix de chercheurs, et a commencé à répliquer ses méthodes sur la plateforme *Bluesky*.

Si les narratifs propagés par *Matriochka* visent majoritairement le gouvernement ukrainien, les contenus mis en ligne ont également ciblé la politique française de soutien à l'Ukraine, des personnalités politiques françaises, ainsi que des thématiques clivantes ou anxiogènes liées à l'immigration, à la sécurité intérieure, à l'économie ainsi qu'à des grands événements comme les Jeux Olympiques et Paralympiques de Paris 2024 (JOP24).

VIGINUM estime que l'objectif de cette campagne reste de décrédibiliser et de saturer les capacités d'investigation des médias, des personnalités et des cellules de *fact-checking* ciblés, tout en espérant que certains de ces contenus pro-russes atteignent une large audience. À ce stade, VIGINUM considère que la capacité du MOI à façonner l'opinion des audiences visées demeure très limitée, et que le succès de certaines de ses opérations repose surtout sur l'attention médiatique qui a pu leur être accordée.

Cette pratique s'apparente à ce que la chercheuse Camille FRANÇOIS qualifiait dès 2020 de « *meta-trolling* », qui renvoie à « des campagnes sur les médias sociaux conçues pour être exposées et couvertes par les médias afin de raviver le débat clivant et chaotique sur l'ingérence russe ».

3. MODES OPÉRATOIRES INFORMATIONNELS CIBLANT L'EUROPE

Depuis la suspension de la diffusion des médias *RT* et *Sputnik* sur le territoire de l'Union européenne le 2 mars 2022, la Fédération de Russie a été contrainte de réorganiser ses capacités de diffusion de ses récits vers le public européen. Alors que des stratégies de contournement des sanctions ont été mises en place par les deux médias d'État transnationaux, VIGINUM a également observé l'apparition de nouveaux médias *web* à destination d'un public ukrainien et européen. En parallèle, le dispositif d'influence russe a également cherché à amplifier, dans le champ informationnel, de fausses manifestations anti-ukrainiennes dans plusieurs capitales européennes, à travers le recrutement d'intermédiaires sur des plateformes en ligne.

3.1. *Voice of Europe* et *Euromore*, deux médias créés pour contourner les sanctions européennes

Le site *Voice of Europe*, actif depuis le printemps 2023, était un média qui promouvait la position de la Russie sur le conflit en Ukraine et dénigrait le gouvernement de Volodymyr ZELENSKY auprès d'audiences occidentales. Le média publiait des interviews de politiciens pro-russes candidats aux élections européennes de juin 2024 et faisait la promotion des partis européens dont la ligne politique était alignée sur les positions de l'État russe. Au-delà de son volet informationnel, le réseau *Voice of Europe* aurait également servi de couverture pour approcher des personnalités politiques européennes favorables à l'arrêt du soutien apporté à l'Ukraine.

Des documents internes de l'Administration présidentielle russe révélés en source ouverte suggèrent que le site était initialement lié à une autre opération d'influence nommée « Une autre Ukraine » (*Drougaïa Ukraïna*), lancée en 2023 et supervisée par le premier vice-directeur de l'AP, Sergueï KIRIENKO. Selon les autorités tchèques, *Voice of Europe* faisait partie d'un projet co-piloté par l'oligarque ukrainien Viktor MEDVEDTCHOUK et par son proche collaborateur Artyom MARTCHEVSKY, producteur de la chaîne *112*.

Le 17 mai 2024, l'Union européenne a suspendu l'accès au site *voiceofeurope[.]com* et placé Viktor MEDVEDTCHOUK et Artyom MARTCHEVSKY sous sanctions pour avoir financé et dirigé *Voice of Europe*. VIGINUM a néanmoins observé d'autres médias *web* aux caractéristiques similaires continuant de promouvoir des récits pro-russes auprès du public européen, parmi lesquels *euromore[.]eu*.

Euromore est un média *web* officiellement basé à Bruxelles créé en 2023, qui se présente comme un site traitant de l'actualité internationale et destiné à un public européen. Le site propose des traductions automatisées de ses articles en 48 langues. Le contenu est publié sous la forme d'articles d'opinion, qui reprennent les déclarations de personnalités politiques européennes pro-russes. Pour autant, le site, qui ne produit aucun contenu original, ne fait qu'agréger du contenu (articles, images et interviews) issu de médias européens ou russes, tels que l'agence de presse *TASS* ou le média *RT*.

Des documents révélés en juin 2024 suggèrent que le site *Euromore* serait financé par *Pravfond*, une organisation russe destinée « aux ressortissants russes vivant à l'étranger » accusée par le service de renseignement extérieur estonien (*Välisluureamet*) d'être liée à l'unité 54777 du service de renseignement militaire russe (GRU). Selon ces mêmes documents, *Euromore* aurait été créé pour cibler spécifiquement l'audience occidentale, en tant « qu'élément de contre-propagande vis-à-vis des médias pro-occidentaux ».

3.2. *Stop Erdogan* et fausses manifestations anti-ukrainiennes

Au mois de mars 2023, VIGINUM a détecté une opération informationnelle impliquant la diffusion, par des comptes *Facebook* présentant des caractéristiques d'inauthenticité, de plusieurs photos de graffitis prises dans différentes rues parisiennes, ainsi que d'une vidéo tournée à proximité de la Halle Saint-Pierre, dans le 18e arrondissement de Paris. La diffusion de ces contenus, publiés sur des groupes *Facebook* destinés aux diasporas turques d'Europe, est intervenue quelques semaines après le séisme ayant provoqué plus de 53 000 victimes en Turquie. Les contenus mettaient en avant des graffitis indiquant par exemple « Stop Islam » et « Alanya Next », ainsi que des individus effectuant des saluts nazis devant une banderole sur laquelle figurait un drapeau ukrainien avec le message suivant : « Erdogan, le tremblement de terre est une rétribution pour les touristes russes ! ».

Selon une enquête menée par un consortium de médias incluant notamment *Le Monde* et le *Centre Dossier*, cette opération aurait fait partie d'une campagne plus large menée par un service de renseignement russe non-précisé. Active depuis *a minima* juillet 2022, cette campagne a consisté en l'organisation de faux rassemblements ou manifestations dans plusieurs capitales d'Europe visant à discréditer l'Ukraine, l'Union européenne ou la Turquie. Des manifestations auraient ainsi été organisées à Paris, à La Haye, à Bruxelles ou encore à Madrid, puis diffusées sur différents comptes *Facebook* et chaînes *YouTube* créés pour l'occasion.



Figure 2. Capture d'écran de la vidéo

Si ces opérations ont nécessité des moyens financiers notables et une coordination entre différents acteurs du dispositif d'influence informationnelle russe, notamment pour le recrutement des individus présents à ces fausses manifestations et la sponsorisation des contenus sur les plateformes, cette campagne particulièrement mal exécutée n'a produit qu'un très faible volume de réactions en ligne.

VIGINUM souligne par ailleurs que le dispositif d'influence informationnelle russe a recouru à plusieurs reprises, pour ce type d'opérations peu sophistiquées, à des sous-traitants et intermédiaires peu formés et facilement remplaçables. Ce procédé permet aux opérateurs de multiplier des opérations à moindre coût et de donner une impression de saturation de l'espace informationnel valorisable auprès de leurs commanditaires, en dépit d'une visibilité quasi nulle.

4. MODES OPÉRATOIRES INFORMATIONNELS CIBLANT L'UKRAINE ET LES TERRITOIRES OCCUPÉS

Dès le déclenchement de la guerre d'agression de la Russie contre l'Ukraine le 24 février 2022, les autorités russes ont cherché à légitimer « l'opération militaire spéciale » auprès de la population ukrainienne à travers de nouveaux médias, notamment dans les territoires actuellement occupés par la Russie. Comme l'a montré une enquête de l'ONG *Reporters sans frontières*, des chaînes de télévision locales pro-russes ont ainsi été lancées dès le mois de juin 2022 dans les *oblasts* ukrainiens de Kherson et de Zaporijjia. À ces chaînes de télévision se sont progressivement ajoutés de nouveaux sites *web* dont l'objectif est de dénigrer le gouvernement ukrainien et de promouvoir les récits du gouvernement russe et de partis politiques sécessionnistes ukrainiens.

4.1. *Portal Kombat*, un MOI ciblant initialement l'Ukraine avant d'étendre ses activités vers l'Europe

Au mois de septembre 2023, VIGINUM a détecté l'existence d'un site *web* pro-russe, *pravda-fr[.]com*, qui diffusait des contenus sur le conflit russo-ukrainien en présentant de manière positive « l'opération militaire spéciale » et en dénigrant l'Ukraine et ses dirigeants auprès d'audiences occidentales, notamment française. Des investigations supplémentaires ont permis de rattacher ce site *web* à un mode opératoire informationnel dénommé *Portal Kombat* par VIGINUM, et dont les opérations informationnelles se sont progressivement étendues de l'Ukraine et des territoires occupés à l'ensemble de l'Europe.

Le MOI *Portal Kombat* repose sur un réseau de plus de 200 sites *web* qui ne produisent aucun contenu original, mais relaient massivement des publications issues de sources pro-russes, notamment des chaînes *Telegram*, des agences de presse ou des sites officiels russes. Au sein de ce réseau, VIGINUM a identifié un écosystème de sites ciblant spécifiquement l'Ukraine, créé à partir d'avril 2022, quelques semaines après le début de l'invasion russe. Sur ces sites, la majeure partie des contenus diffusés vise à amplifier le ressentiment des populations locales russophones à l'encontre des autorités ukrainiennes et à informer sur les opérations militaires en cours, comme en témoigne la rubrique « correspondants militaires » de ces sites. Ces derniers constituent donc de véritables « caisses de résonance » du dispositif d'influence numérique russe, et ce, suivant un maillage informationnel méticuleux du territoire ukrainien.

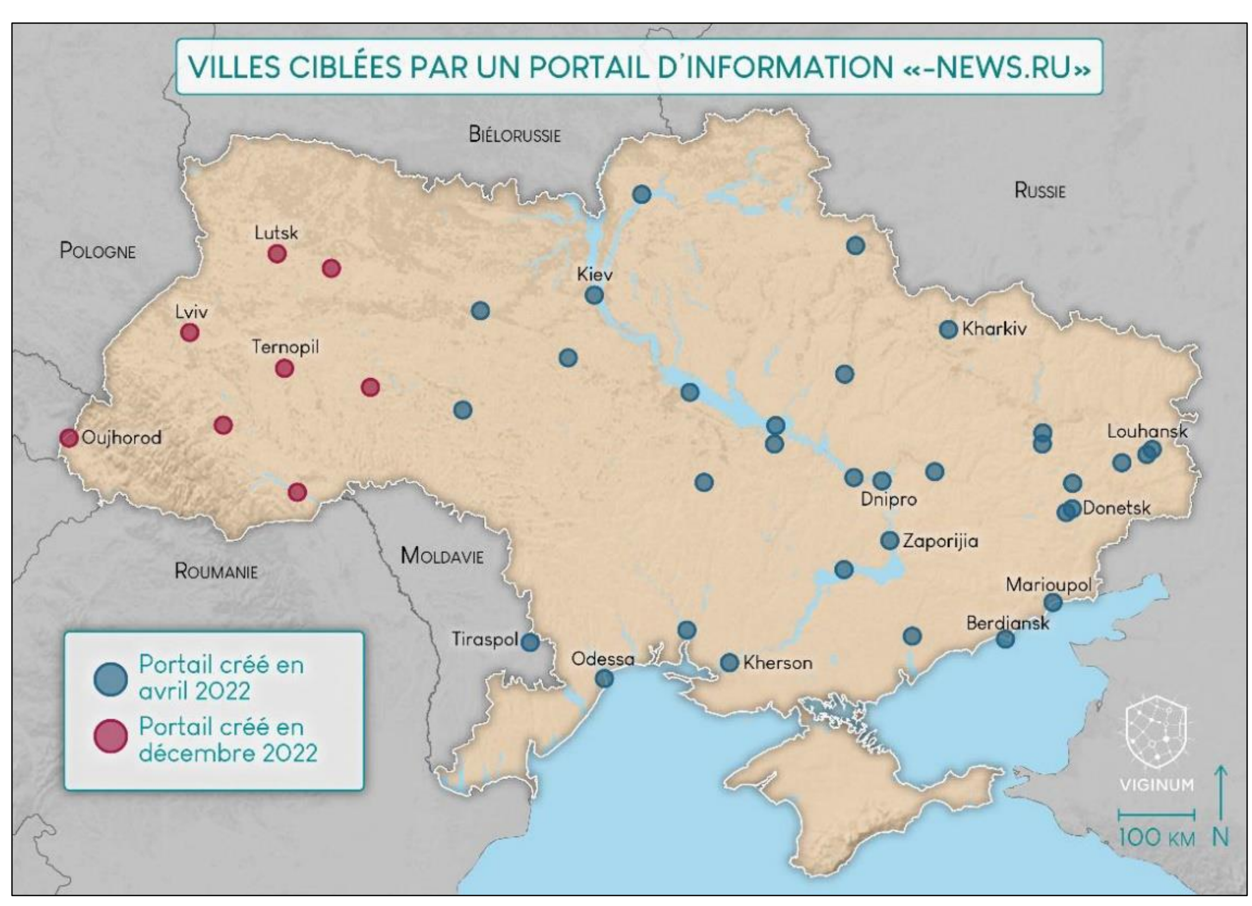


Figure 3. Villes ukrainiennes ciblées par des sites du MOI Portal Kombat

Les investigations de VIGINUM ont révélé l'implication directe d'une entreprise de développement *web* russe nommée *TigerWeb* et basée en Crimée, dans la création et l'administration de ces sites. Cette entreprise, gérée notamment par le citoyen russe Evgueni CHEVTCHENKO, développe et maintient des sites *web* depuis au moins 2013. Evgueni CHEVTCHENKO a travaillé comme chef de projet au sein de *Krymtechnologii*, une entreprise régionale d'État (désormais privatisée) liée au ministère de la Politique intérieure, de l'information et de la communication de la République russe de Crimée.

En février 2024, les ministres des Affaires étrangères français, polonais et allemand ont dénoncé conjointement le MOI *Portal Kombat*. Depuis cette exposition publique, VIGINUM a observé une extension du réseau et la création de nouveaux noms de domaine et de sous-domaines ciblant l'ensemble des États membres de l'Union européenne, plusieurs pays d'Afrique et d'Asie, ainsi que des personnalités politiques françaises, à l'instar du président de la République Emmanuel MACRON. Les différentes évolutions de *Portal Kombat*, parfois corrélées à des événements comme les JOP2024 ou des échéances électorales (élections européennes, élections en Moldavie, etc.), témoignent de la persistance du MOI et de la volonté du dispositif d'influence russe de saturer l'espace informationnel ukrainien, même à une échelle très locale.

4.2. *Mriya*, un média lié à un parti politique sécessioniste ukrainien

Depuis le milieu des années 2010, le dispositif d'influence informationnelle russe utilise de nombreuses chaînes *Telegram* russophones pour diffuser des contenus à destination d'audiences ukrainiennes, notamment celles situées dans les territoires actuellement occupés par la Russie. C'est le cas de « *Mriya* » (« le rêve », en ukrainien)[2], un média agrégateur de chaînes *Telegram* russophones désormais inactif, qui disposait également d'un site enregistré à la fin de l'année 2022. Si le média affirmait avoir été créé par « une équipe […] qui se bat quotidiennement pour mettre fin à la folie qui sévit en Ukraine aujourd'hui », il était en fait composé d'influenceurs ukrainiens favorables aux intérêts russes[3].

Les membres du média *Mriya* diffusaient des contenus manifestement trompeurs sur leurs chaînes *Telegram* et animaient des émissions dénigrant le gouvernement de Volodymyr ZELENSKY. À plusieurs reprises, les publications de *Mriya* et de ses blogueurs ont bénéficié d'une amplification par des *bots* du MOI *RRN*. En parallèle de leur activité médiatique, certains influenceurs de *Mriya* seraient intervenus au moins une fois dans des manifestations anti-Ukraine et anti-OTAN organisées dans des villes européennes, possiblement en partenariat avec une agence de communication moldave déjà impliquée dans une tentative d'ingérence numérique en Israël.

Les investigations menées par VIGINUM ont permis d'établir que « *Mriya* » était la vitrine médiatique d'un projet politique séparatiste nommé le « Bureau de représentation du peuple ukrainien » (BRPU), dont le site est inactif à ce jour. Fondé par l'activiste ukrainien Dmitry VASILETS, l'objectif du BRPU était de promouvoir un « plan pour la paix » comprenant le renversement de Volodymyr ZELENSKY et l'organisation de « référendums d'autonomie » dans toutes les régions d'Ukraine. VIGINUM a par ailleurs mis en évidence la volonté des membres du BRPU d'obtenir des soutiens politiques à l'échelle internationale, en prenant notamment contact avec des parlementaires de l'Union européenne et de plusieurs pays des Balkans.

D'après une fuite de documents internes de la société russe *ASP*, les chaînes *Telegram* de certains membres du BRPU, dont Dmitry VASILETS et Maksim CHIKHALIEV (administrateur de la chaîne *@sheyhtamir1974*), auraient été utilisées comme vecteurs de diffusion par le « Centre S », une cellule interne d'*ASP* qui serait chargée, selon le DoJ américain, de mener des opérations informationnelles ciblant l'Ukraine.

5. MODES OPÉRATOIRES INFORMATIONNELS CIBLANT LE CONTINENT AFRICAIN

L'invasion de l'Ukraine a renforcé l'isolement de la Russie vis-à-vis des puissances occidentales, et l'a contrainte à rechercher de nouveaux partenariats sur la scène internationale, notamment sur le continent africain. Ce pivot stratégique vers l'Afrique, inscrit dans le Concept de politique étrangère de la Fédération de Russie de 2023, s'est évidemment matérialisé par le déploiement du groupe

---

[2] Le MOI *Mriya* décrit dans cette partie n'est, à la connaissance de VIGINUM, pas lié au prétendu « collectif artistique ukrainien » éponyme ayant revendiqué la pose de cercueils devant la Tour Eiffel au mois de juin 2024.

[3] Les chaînes *Telegram* de ces influenceurs sont notamment : *@sheyhtamir1974*, *@tarik_nezalejko*, *@VasiletsDmitriy*, *@Onishchenko001* et *@AleksandrSemchenko*.

paramilitaire Wagner dans plusieurs États d'Afrique avec lesquels la France avait une histoire politique et des accords de défense. Dans ce contexte, VIGINUM observe régulièrement des opérations informationnelles accusant la France et l'Ukraine de financer des groupes armés terroristes en Afrique pour déstabiliser les régimes alliés de la Russie, ou accusant l'Ukraine de chercher à impliquer l'Afrique dans « sa guerre ».

5.1. Projet *Lakhta* et campagne sur un prétendu envoi de citoyens africains sur le front ukrainien

Créé en 2013 par l'homme d'affaires russe Evgueni PRIGOJINE, le projet *Lakhta*, aussi connu sous le nom d'*Internet Research Agency* (IRA), est une structure semi-clandestine chargée de préparer et de conduire des opérations d'influence vers l'étranger. Particulièrement actif sur le continent africain, le projet *Lakhta* a été à l'origine de nombreuses campagnes informationnelles d'appui au déploiement du groupe Wagner ciblant la France, notamment en République centrafricaine ou dans la bande sahélo-saharienne.

Depuis la mort de Evgueni PRIGOJINE le 23 août 2023, la structure poursuit ses activités, sans qu'il soit possible de déterminer l'identité de son nouveau commanditaire. Selon un article du *New York Times* publié en septembre 2023, le projet *Lakhta* pourrait être passé sous le contrôle du Service de renseignement extérieur russe (SVR).

Dans le cadre de la guerre d'agression de la Russie en Ukraine et de la stratégie de développement de la présence russe sur le continent africain, le projet *Lakhta* a mené plusieurs campagnes informationnelles visant à dénigrer l'image de la France. Pour ce faire, le MOI a notamment exploité un réseau de plusieurs dizaines de faux comptes *X* et de pages *Facebook* administrés depuis des pays d'Afrique francophone, actifs depuis la fin de l'année 2021 et suspendues par *Meta* au cours de l'été 2024. L'une de ces campagnes, ciblant les diasporas africaines de France, s'est déroulée sur *Facebook* et sur le *web* à travers plusieurs opérations conduites entre les 5 et 20 avril 2024. Elle a consisté à accuser le gouvernement français de préparer l'envoi d'un contingent d'immigrés africains pour combattre en Ukraine.



Figure 4. Captures d'écran de publications sponsorisées de pages du projet Lakhta

Cette campagne a utilisé des tactiques, techniques et procédures propres au projet *Lakhta*, déjà observées à de nombreuses reprises dans plusieurs États africains, notamment en République centrafricaine, mêlant l'utilisation de comptes inauthentiques sur les plateformes pour diffuser de fausses informations, la diffusion contre rémunération d'articles dans des médias africains, et l'organisation d'événements dans le champ physique, comme de fausses manifestations.

Après plusieurs mois d’interruption, cette campagne a été relancée entre le 24 janvier et le 14 février 2025, accusant une nouvelle fois la France de chercher à mobiliser secrètement des citoyens africains, notamment camerounais, pour combattre en Ukraine. Elle a mobilisé plusieurs pages *Facebook* et comptes *X* (pour certains actifs depuis plusieurs années) qui ont diffusé des captures d’écran d’une fausse annonce de recrutement de *France Travail* pour « des analystes de bases de données et des ingénieurs en explosifs au Cameroun ».

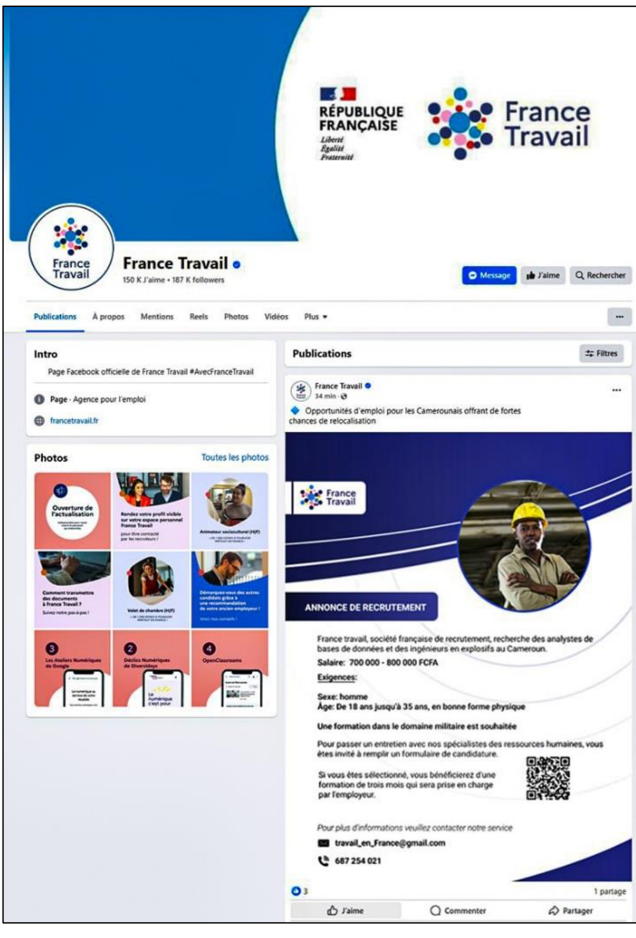


Figure 5. Fausse capture d'écran d'une annonce d'emploi de France Travail

En parallèle, une vidéo d’un prétendu témoignage d’un citoyen camerounais ayant répondu à l’offre d’emploi a été diffusée par une page *Facebook* affiliée au projet *Lakhta*. La fausse annonce comportait également un code QR redirigeant vers un faux site sur lequel figure un formulaire de recrutement. Par ailleurs, des pages *Facebook* affiliées au projet *Lakhta* ont diffusé des contenus sponsorisés affirmant que l’Ukraine chercherait à former, en République de Côte d’Ivoire, une « légion étrangère » constituée de citoyens ivoiriens pour l’envoyer sur le front contre la Russie.

Si VIGINUM considère l’impact de cette campagne comme faible, elle illustre l’une des spécificités des campagnes du projet *Lakhta*, qui combinent des actions dans les champs informationnel (publication d’articles rémunérés, publicités en ligne, animation de fausses pages *Facebook*) et physique (organisation de faux rassemblements).

VIGINUM observe par ailleurs que les allégations manifestement inexactes ou trompeuses diffusées par le projet *Lakhta* à l’encontre de la France font écho aux pratiques réelles de la Russie, déjà mise en cause pour avoir enrôlé de force des étudiants et immigrés africains pour combattre en Ukraine.

À PROPOS DE VIGINUM



Créé le 13 juillet 2021 et rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation.

Ce service technique et opérationnel de l'État a pour mission de détecter et caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN

Crédit photo couverture : Photo de Sylwia Bartyzel sur Unsplash.